WIKIPEDIA

Wiener's attack

The **Wiener's attack**, named after cryptologist Michael J. Wiener, is a type of cryptographic attack against RSA. The attack uses the continued fraction method to expose the private key *d* when *d* is small.

Contents

Background on RSA

Fictional characters Alice and Bob are people who want to communicate securely. More specifically, Alice wants to send a message to Bob which only Bob can read. First Bob chooses two primes *p* and *q*. Then he calculates the RSA modulus *N* = *pq*. This RSA modulus is made public together with the encryption exponent *e*. *N* and *e* form the public key pair *(e,N)*. By making this information public, anyone can encrypt messages to Bob. The decryption exponent *d* satisfies $ed = 1 \bmod \lambda(N)$, where $\lambda(N)$ denotes the Carmichael function, though sometimes $\varphi(N)$, the Euler's phi function, is used (note: this is the order of the multiplicative group $\mathbb{Z}_N^*$, which is not necessarily a cyclic group). The encryption exponent *e* and $\lambda(N)$ also must be relatively prime so that there is a modular inverse. The factorization of *N* and the private key *d* are kept secret, so that only Bob can decrypt the message. We denote the private key pair as *(d, N)*. The encryption of the message *M* is given by $C \equiv M^e \bmod N$ and the decryption of cipher text C is given by $C^d \equiv (M^e)^d \equiv M^{(ed)} \equiv M \bmod N$ (using Fermat's little theorem).

Using the Euclidean algorithm, one can efficiently recover the secret key *d* if one knows the factorization of *N*. By having the secret key *d*, one can efficiently factor the modulus of *N*.[1]

Small private key

In the RSA cryptosystem, Bob might tend to use a small value of *d*, rather than a large random number to improve the RSA decryption performance. However, Wiener's attack shows that choosing a small value for *d* will result in an insecure system in which an attacker can recover all secret information, i.e., break the RSA system. This break is based on Wiener's Theorem, which holds for small values of *d*. Wiener has proved that the attacker may efficiently find *d* when $d < \frac{1}{3}N^{\frac{1}{4}}$.[2]

Wiener's paper also presented some countermeasures against his attack that allow fast decryption. Two techniques are described as follows.

Choosing large public key: Replace e by e', where $e' = e + k \cdot \lambda(N)$ for some large of k. When e' is large enough, i.e. $e' > N^{\frac{3}{2}}$, then Wiener's attack can not be applied regardless of how small d is.

Using the Chinese Remainder Theorem: Suppose one chooses d such that both $d_p = d \bmod (p-1)$ and $d_q = d \bmod (q-1)$ are small but d itself is not, then a fast decryption of C can be done as follows:

1. First compute $M_p \equiv C^{d_p} \bmod p$ and $M_q \equiv C^{d_q} \bmod q$.
2. Use the Chinese Remainder Theorem to compute the unique value of $M \in \mathbb{Z}_{\mathbb{N}}$ which satisfies $M \equiv M_p \bmod p$ and $M \equiv M_q \bmod q$. The result of M satisfies $M \equiv C^d \bmod N$ as needed. The point is that Wiener's attack does not apply here because the value of $d \bmod \lambda(N)$ can be large. [3]

How Wiener's attack works

Note that

$$\lambda(N) = \operatorname{lcm}(p-1, q-1) = \frac{(p-1)(q-1)}{G} = \frac{\varphi(N)}{G}$$

where $G = \gcd(p-1, q-1)$

Since

$$ed \equiv 1 \pmod{\lambda(N)},$$

there exists an integer K such that

$$ed = K \times \lambda(N) + 1$$

$$ed = \frac{K}{G}(p-1)(q-1) + 1$$

Defining $k = \dfrac{K}{\gcd(K,G)}$ and $g = \dfrac{G}{\gcd(K,G)}$, and substituting into the above gives:

$$ed = \frac{k}{g}(p-1)(q-1) + 1.$$

Divided by dpq:

$$\frac{e}{pq} = \frac{k}{dg}(1-\delta), \text{where } \delta = \frac{p+q-1-\frac{g}{k}}{pq}.$$

So, $\dfrac{e}{pq}$ is slightly smaller than $\dfrac{k}{dg}$, and the former is composed entirely of public information. However, a method of checking and guess is still required. Assuming that $ed > pq$ (a reasonable assumption unless G is large) the last equation above may be written as:

$$edg = k(p-1)(q-1) + g$$

By using simple algebraic manipulations and identities, a guess can be checked for accuracy. [1]

Wiener's theorem

Let $N = pq$ with $q < p < 2q$. Let $d < \frac{1}{3}N^{\frac{1}{4}}$.
Given $\langle N, e \rangle$ with $ed \equiv 1 \pmod{\lambda(N)}$, the attacker can efficiently recover d.[2]

Example

Suppose that the public keys are $\langle N, e \rangle = \langle 90581, 17993 \rangle$
The attack shall determine d.
By using Wiener's Theorem and continued fractions to approximate d, first we try to find the continued fractions expansion of $\frac{e}{N}$. Note that this algorithm finds fractions in their lowest terms. We know that

$$\frac{e}{N} = \frac{17993}{90581} = \cfrac{1}{5 + \cfrac{1}{29 + \cdots + \cfrac{1}{3}}} = [0, 5, 29, 4, 1, 3, 2, 4, 3]$$

According to the continued fractions expansion of $\frac{e}{N}$, all convergents $\frac{k}{d}$ are:

$$\frac{k}{d} = 0, \frac{1}{5}, \frac{29}{146}, \frac{117}{589}, \frac{146}{735}, \frac{555}{2794}, \frac{1256}{6323}, \frac{5579}{28086}, \frac{17993}{90581}$$

We can verify that the first convergent does not produce a factorization of N. However, the convergent $\frac{1}{5}$ yields

$$\varphi(N) = \frac{ed-1}{k} = \frac{17993 \times 5 - 1}{1} = 89964$$

Now, if we solve the equation

$$x^2 - ((N - \varphi(N)) + 1)\,x + N = 0$$
$$x^2 - ((90581 - 89964) + 1)\,x + 90581 = 0$$
$$x^2 - 618x + 90581 = 0$$

then we find the roots which are $x = 379; 239$. Therefore we have found the factorization

$$N = 90581 = 379 \times 239 = p \times q.$$

Notice that, for the modulus $N = 90581$, Wiener's Theorem will work if

$$d < \frac{N^{\frac{1}{4}}}{3} \approx 5.7828.$$

Proof of Wiener's theorem

The proof is based on approximations using continued fractions.[2][4]
Since $ed = 1 \bmod \lambda(N)$, there exists a k such that $ed - k\lambda(N) = 1$. Therefore

$$\left|\frac{e}{\lambda(N)} - \frac{k}{d}\right| = \frac{1}{d\lambda(N)}.$$

Let $G = \gcd(p-1, q-1)$, note that if $\varphi(N)$ is used instead of $\lambda(N)$, then the proof can be replaced with $G = 1$ and $\varphi(N)$ replaced with $\lambda(N)$.

Then multiplying by $\frac{1}{G}$,

$$\left|\frac{e}{\varphi(N)} - \frac{k}{Gd}\right| = \frac{1}{d\varphi(N)}$$

Hence, $\frac{k}{Gd}$ is an approximation of $\frac{e}{\varphi(N)}$. Although the attacker does not know $\varphi(N)$, he may use N to approximate it. Indeed, since

$\varphi(N) = N - p - q + 1$ and $p + q - 1 < 3\sqrt{N}$, we have:

$$|p + q - 1| < 3\sqrt{N}$$
$$|N - \varphi(N)| < 3\sqrt{N}$$

Using N in place of $\varphi(N)$ we obtain:

$$\left|\frac{e}{N} - \frac{k}{Gd}\right| = \left|\frac{edG - kN}{NGd}\right|$$

$$= \left|\frac{edG - k\varphi(N) - kN + k\varphi(N)}{NGd}\right|$$
$$= \left|\frac{1 - k(N - \varphi(N))}{NGd}\right|$$
$$\leq \left|\frac{3k\sqrt{N}}{NGd}\right| = \frac{3k\sqrt{N}}{\sqrt{N}\sqrt{N}Gd} \leq \frac{3k}{d\sqrt{N}}$$

Now, $k\lambda(N) = ed - 1 < ed$, so $k\lambda(N) < ed$. Since $e < \lambda(N)$, so $k\lambda(N) < ed < \lambda(N)d$, then we obtain:

$$k\lambda(N) < \lambda(N)d$$
$$k < d$$

Since $k < d$ and $d < \frac{1}{3}N^{\frac{1}{4}}$. Hence we obtain:

$$(1) \left|\frac{e}{N} - \frac{k}{Gd}\right| \leq \frac{1}{dN^{\frac{1}{4}}}$$

Since $d < \frac{1}{3}N^{\frac{1}{4}}$, $2d < 3d$, then $2d < 3d < N^{\frac{1}{4}}$, we obtain:

$$2d < N^{\frac{1}{4}}, \text{ so (2) } \frac{1}{2d} > \frac{1}{N^{\frac{1}{4}}}$$

From (1) and (2), we can conclude that

$$\left|\frac{e}{N} - \frac{k}{Gd}\right| \leq \frac{3k}{d\sqrt{N}} < \frac{1}{d \cdot 2d} = \frac{1}{2d^2}$$

If $\left|x - \frac{a}{b}\right| < \frac{1}{2b^2}$, then $\frac{a}{b}$ is a convergent of x, thus $\frac{k}{d}$ appears among the convergents of $\frac{e}{N}$. Therefore the algorithm will indeed eventually find $\frac{k}{Gd}$.

References

1. L. Render, Elaine (2007). Wiener's Attack on Short Secret Exponents. (http://personalpages.manchester.ac.uk/postgrad/elaine.render/mathtoday.pdf.)
2. Boneh, Dan (1999). Twenty Years of attacks on the RSA Cryptosystem. Notices of the American Mathematical Society (AMS) 46 (2). (http://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf)
3. Cui, Xiao-lei (2005). Attacks On the RSA Cryptosystem. (https://web.archive.org/web/20190512142109/https://pdfs.semanticscholar.org/ce82/c0d989816f52f64a012e3100f426f29964db.pdf)
4. Khaled Salah, Imad (2006). Mathematical Attacks on RSA Cryptosystem. Journal of Computer Science 2 (8)). pp. 665-671. (http://www.scipub.org/fulltext/jcs/jcs28665-671.pdf.)

Further reading

- Coppersmith, Don (1996). Low-Exponent RSA with Related Messages. Springer-Verlag Berlin Heidelberg. (http://portal.acm.org/citation.cfm?id=1754497)
- Dujella, Andrej (2004). Continued Fractions and RSA with Small Secret Exponent. (https://arxiv.org/PS_cache/cs/pdf/0402/0402052v1.pdf)
- Python Implementation of Wiener's Attack. (https://sagi.io/2016/04/crypto-classics-wieners-rsa-attack/)
- R. Stinson, Douglas (2002). *Cryptography Theory and Practice* (2e ed.). A CRC Press Company. pp. 200–204. ISBN 1-58488-206-9.